Managing Technological Vulnerability of Urban Dwellers: Analysis, Trends, and Solutions

Lindsay J. Robertson, Albert Munoz, and Katina Michael, *Senior Member, IEEE*

***Abstract*—Urban dwellers are increasingly dependent on technological systems to supply goods and services essential for their way of life. Such dependence incurs vulnerability in situations when these goods and services are not available. The systems supplying these essentials are known to have many loci of failure. We consider the exposure of a technological system in terms of the number and type of loci of failure and present this as a metric of urban dweller vulnerability. Such a metric captures the vulnerability to the nonavailability of the specific goods or services provided by a particular technological system. By selecting from goods and services commonly required, this article identifies a representative range of essential goods and services provided to urban-dwelling individuals by technological systems, and examines the nature and extent of exposure associated with each system. Based upon the descriptions of these technological systems, this article classifies the contributors to each technological system's exposure into a small number of categories. The analysis allows the inference of generalized approaches for reducing each category of exposure, and hence vulnerability. Thus, a theory of exposure can be used to inform engineering management approaches applicable to end-user vulnerability reduction, and to identify the feasibility of less exposed technological systems.**

***Index Terms*—Exposure, personal security, risk, technology, vulnerability.**

I. Introduction

A. Technological Dependence

THE PERSON living in a city apartment is generally not practically able to gather firewood and use it for cooking; he/she depends on a capability to purchase processed food and has little or no land for practical waste disposal. With the development of greater diversity in geographic, economic, and social categories, comes greater diversity in each group's vulnerability to system failures. The persons living in a high-density urban setting are no exception, as they subsist under the regulatory constraints typical of a modern city. The urban dweller in a typical small city is specifically dependent on technological systems to provide goods and services that enable their way of life. Such an urban dweller is, therefore, vulnerable to the nonavailability of these goods and services, and is exposed to the possibility of failure of the systems that progressively create and distribute even such basic services as sewage removal and water supply.

The principle [1] that "solutions breed new problems" may be seen as paradoxical. New processes intended to resolve prior vulnerabilities now increase our vulnerability are those which historically have increased the wellbeing of so many. For example, Norman Borlaug's revolutionizing of agriculture [2] allowed billions to be fed where previous methods would have failed to do so. Similarly, James Watt's [3] translation of science into practical power from fossil fuel, and Henry Ford's [4] innovations that brought motor vehicles within the economic means of most, and the combined innovations of IT hardware and the Internet have brought a wealth of information and communication options. Yet, these advances create situations where urban dwellers are vulnerable to last-mile communication and power supply failures, work capabilities, access to essential foods, medical supplies, sources of water, sewage disposal, etc.

B. Risk, Exposure, and Vulnerability

Risk analysis, which categorizes hazard-probability (i.e., outcome-severity list items) is considered a mature disciple and is undoubtedly useful, but suffers from some shortcomings. One such example is the reliance on assignments of hazard probability. Particularly within homogeneous systems, sophisticated approaches to calculating the propagation of component risks and their effect on system risk [5], [6] have been proposed, but also depend on the input values of "risk." Even where historical data can inform such indices the data is by definition not predictive, and for many situations real historical data is unavailable.

We have instead assessed the vulnerability presented by a technological system, noting that components of any specific technological system inevitably represent weaknesses that are exposed to threats that can potentially cause technological systems failure. Such failures result in the nondelivery of goods or services as designed. Any threat to a technological system is only significant if it aligns with a specific weakness of that system, conversely, every weakness can potentially be targeted by a range of threats. Thus, the configuration of a technological system's weaknesses determines its "exposure." Some threats may have statistical probabilities

Manuscript received October 30, 2019; revised January 26, 2020 and February 17, 2020; accepted February 18, 2020. Date of publication February 23, 2020; date of current version March 11, 2020. This work was supported in part by the Australian Government Research Training Program (RTP) Scholarship. This article was recommended for publication by Associate Editor E. Scornavacca. *(Corresponding author: Lindsay J. Robertson.)*

Lindsay J. Robertson is with the SCIT, University of Wollongong, Wollongong, NSW 2522, Australia (e-mail: lindsay@tech-vantage.com).

Albert Munoz is with the Faculty of Business, University of Wollongong, Wollongong, NSW 2522, Australia.

Katina Michael is with the School for the Future of Innovation in Society and the School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ 85287 USA.

Digital Object Identifier 10.1109/TTS.2020.2975806

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

but these will approach a value of 1.0 over long timeframes, and intelligently (mis)guided threats must be considered to always have a probability of 1.0. These observations suggest that the configuration of a technological system and its weaknesses are actually the most important factor in determining the vulnerability that it incurs for users of its outputs, and must be considered independently of the reliability of components or any assessment of the probability of some specific hazard's occurrence.

If a service-level output from a technological system is defined, it is possible to describe the complete system's output as a Boolean value and it is possible to derive that value from a Boolean expression that models process and stream availabilities as Boolean values, and thus represents the complete system. Within such an expression, AND functions describe cases where an intermediate stream is generated when input streams and functional processes are available. Correspondingly, OR functions describe cases where alternative processes or streams can supply the required functionality. A truth table representation of all cases where single failures cause output failure to be constructed, and similarly allows a summation of the number of cases where dual failures cause output failure, etc. These summations can be represented in the form $\{E_1, E_2, E_3, \ldots\}$, where E_1 is the number of cases where a single stream or process failure will cause output failure, E_2 is the number of cases where two failures (neither contributing to E_1) will cause output failure, etc. The metric $\{E_1, E_2, E_3, \ldots\}$ has previously [7] been shown to be a representation of the exposure of the technological system from which it is derived, and a valid measure of the vulnerability imposed on the user. It has been proposed [8] that whenever a system is sufficiently complex, failure is inevitable. However, a quantitative approach that is directly mapped to the system under consideration offers opportunities for both identifying and evaluating potential improvements.

The direct system mapping allows both peer review, and an objective assessment of completeness that contribute confidence of reproducibility. This definition of exposure is, therefore, a more finely grained and quantitative approach to the common concept of exposure as proposed by [9] and others. While an exposure metric is calculated for a specific technological system supplying a single individual, the metric also applies to every individual supplied by that technological system. Noting the human value of the security, and also the large and increasing population who are dependent on technological systems is valuable to quantify levels of individual vulnerability.

C. Value of Vulnerability Reduction in Managing Innovations

Currently, 50% of the world's total population lives in urban contexts, and is projected to rise to 75% by 2050 [10]. Others live in vastly different (rural/village) situations and their circumstances generate both opportunities for reduced vulnerability, and paradoxically cases where they are more vulnerable than urban dwellers. This article considers only the urban dwellers and primarily assumes a western-style city, noting that this type of settlement is both a large, and increasing segment of the world's total population. For those in such urban environments, a way of life depends on technological systems, and value will be placed on the security of that way of life. It is thus valuable to consider the technological vulnerabilities of representative cases, and to question whether generalized approaches to the reduction of technological vulnerability are possible and feasible. In this way, we propose that those tasked with managing innovations and critical engineering systems, consider from the outset how the systems they are creating hold up in terms of risk(s) to society. Once widely deployed, it becomes very difficult to make changes to system exposures that influence end-user vulnerability. Consider, for example, a point-of-sale (POS) terminal that has been created to provide end users with convenience in paying for a good without cash. If those terminals have been deployed to thousands of merchants, relying solely on electricity, then without power the units become inoperable. In such an example, redundant power sources could have been considered from the outset.

This article addresses vulnerabilities to urban dweller's way of life through engineering management, technology systems, and the reduction of end-user vulnerability. Controlling exposure of systems at the design stage reduces end-users' vulnerability. It is acknowledged that technological failures affecting the target group may also affect other groups, and categories of technological failures have the potential to represent a threat to all life but the examination of such "existential threats" is outside the scope of this article.

II. Methodology

A. Analysis of Exposure of Selected Technological Systems

This article considers the analysis, trends, and solutions to technological vulnerabilities. In order to draw any conclusions regarding the overall technological vulnerability of an "urban dweller," analysis of actual technological systems supplying essential goods/services to such a dweller is required. Only essential services are considered, and we propose simply that the supply of a type of good or service may be considered "essential" if significant and unplanned lifestyle changes will be required in response to a nonavailability. This definition also avoids any requirement to rank the significance of systems or examples. An urban dweller may be expected to use a significant variety of specific essential goods and services over an extended period, however, we observe that many of these specific requirements differ only in the detail of the technological systems used to deliver them—and that common subsystems (such as water and power supplies) contribute to the supply of many specific goods or services.

An initial candidate list of essential goods or services was developed by reviewing the activities of a city apartment dweller over a period of weeks and observing whether a lack would cause significant lifestyle change. An inspection allowed items within this candidate list to be grouped based on the similarity of the technological systems required and further inspection allowed these to be associated with groupings, such as "services that accumulated

feedstock from many sources and locally processed" or "central goods creation followed by widespread dissemination" or "person to person communications requiring common intelligibility."

From these categorizations, previous work [11] allowed the identification of a number of technological systems that are representative of the goods and services essential to the lifestyle of typical urban dwellers. For each, implementations within several cities were researched using publicly available information. Our review of technological systems used to supply the selected goods or services across several cities, showed that although systems were not identical, there was a high level of commonality and thus it was possible to examine the technological systems that typically supply each of these goods or services, and the nature and extent of exposure associated with each is identified and described. The scope of examples, the inclusion of common subsystems, and the number of other specific systems that bear close similarity to the studied examples, are sufficiently broad and representative to provide the foundation for identification of categories of vulnerability, and ultimately for the proposal of generic approaches to the reduction of vulnerability.

B. Validity of Example Analysis

The technological system descriptions are considered for a timeframe within which neither maintenance nor component replacement is needed (i.e., an "operational timeframe"). In longer timeframes, it would be necessary to consider the situations where technological systems require maintenance, and hence require not only replacement parts but also personnel capable of installation and recommissioning. In yet longer timeframes, we must also consider the case of technological subsystems reaching the end of their operational life and requiring replacement. Replacement includes the sourcing of basic materials, the availability of designs, manufacture of parts, skilled assembly, and recommissioning tasks.

Maintenance needs are typically more extensive than operational needs and remanufacture of operational subsystems incurs many more operations than those associated with operational timeframes. Nevertheless, maintenance and replacement timeframes are also generally longer than operational timeframes and options for their management. Even for complex systems, it is commonly observed that the time required to establish manufacturing facilities for replacement systems is less than the expected time to failure for the systems. Buffering (of maintenance and replacement subsystems does not reduce the maintenance or replacement timeframe exposures to depletion of essential basic resources (environmental and raw materials issues), nor to skilled personnel, nor to the existence of information required. This issue has been explored in more detail by others [12]. The analyses have intentionally selected cases that span a range of end-user needs and technological system types. Collectively, these are considered to illustrate a broad span of need-types for a representative urban user. Each of the example technological systems include distinctive features that contribute to the user's vulnerability. The investigation has highlighted a range of specific system exposure points.

C. Identification of Categories of Vulnerability

The cases described in this article are considered representative of a large number of specific goods and services commonly supplied to individuals, but will vary in detail. While the reduction in the vulnerability of any one technological system is valuable, qualitatively higher value can be targeted if specific categories of vulnerability can be identified, described, and associated with generic reduction approaches. In the process of reviewing the specific contributors to exposure for each of the cases, we assigned functional descriptions to each system, subsystem and major component (e.g., high-value, small volume goods, created centrally and distributed or complex-but-widely available components). The functional descriptions allowed grouping and categorization of vulnerabilities and has suggested that a limited range of categories can indeed be identified and thus generic approaches to reduced vulnerability can be proposed.

III. Case Descriptions and Walkthroughs

To consider levels of technological vulnerability and options for reduction, it is first necessary to identify and analyze technological systems commonly used in the supply of a range of essential goods and services. We present examples across a spectrum of high and low-tech systems, related to multiple levels of the Maslow [13] hierarchy of needs, and encompassing technology systems that include aggregation, processing, and distribution functions. This selection illustrates exposure levels and characteristics across a broad range of systems. Specifically, the selected examples cover the provision of common needs (e.g., food), health-related issues (e.g., sewage disposal and medicine), energy/transport, and the information communication. While only summary detail is provided for each, system descriptions allow the categorization of exposures and technological configuration contributions to vulnerability.

A. Sewage Disposal

Without a working sewage disposal system, an apartment becomes effectively uninhabitable, and public health consequences beyond the apartment will manifest within a short period (though the consequences for the sewage system operator may be much smaller). For this example, the service is the sanitary removal of human waste, on an "as required basis," via the lavatory installed in a multistory apartment (a typical urban setting) and resulting in the discharge of environmentally acceptable water to waterways, and of solid waste of environmentally acceptable specifications to landfill. As with many subsystems close to the point of end user, apartment subsystems contribute significantly to the E_1 value, representing single points of failure. The gravity-fed sewage pipework and pumping system makes smaller contributions to the E_1 and E_2 values. The sewage treatment plant includes multiple operations that cannot be bypassed without affecting the purpose of the system (e.g., the discharge of acceptable quality

waste) and hence a major contributor to the numerical exposure of the sewage system is the multiple sequential stages of treatment needed to transform the sewage into streams that can be discharged without environmental damage.

B. Work Information

The storage and transmission of information generally are foundational to civilization, the recording of medical, veterinary and agricultural knowledge, teaching of engineering, recording of contracts and commitments, recording of family history information, cartography, cultural records, and chemical information is essential. This example considers a requirement to store and retrieve, view, edit, and share information in the context of daily work. The definition of service delivery for this example implies that the complex information is able to be read, seen, and updated by more than one party, before being read by the intended recipient. This example assumes the use of two local workstation operations, and an Internet connection between them. The Internet system includes the routers, power supplies, and fiber connections to regional peering points, routers power supplies, and connections to acceptable access points, with power supplies, signal boosters, and shielding systems. The operations local to both of the end-users contribute significantly to the E_1 value. Contributors include the power supply to two computers and routers, data wiring via the telephone system, and to two local Internet points of presence (POPs) and power supply wiring to the local substation.

C. Local Fuel Supply

Users have limited capability to store, and no practical means to manufacture fuel, yet distances and loads required for commuting and acquiring goods are commonly beyond reasonable walking/carrying capabilities. For this example, the service is the supply of petrol into a user's vehicle, at a staffed petrol station. The service considers the operation of the dispensing pumps, local fuel storage tanks, metering, and transactional services, the refilling of the underground tanks from fuel stored in national-reserves and the production from crude sources of those national reserves. The supply of bulk fuel is assumed to be available from only one source. The station is unlikely to have duplicated power feeders from the nearest substation. The local substation will probably have at least dual in-feeds from the national grid and so there is no need to consider power supply security beyond that point. The assumption is made that an electronic payment system is used, requiring communication between the seller's EFTPOS terminal and the acquirer's bank, then with the purchaser's bank and finally a transfer to the merchant's bank. Each monetary transaction process requires hardware, software, and power supplies. Intermediate communications are via Internet services. A staffed station is assumed and hence staff facilities, including sewage and water supply are required. The systems at the forecourt make a significant contribution to the total exposure, it is useful to note that metering and control systems for pumps contribute as well as the actual pumps. The financial transaction system, i.e., EFTPOS and banking, affect all examples that rely on a retailer to consumer transaction and is a major contributor of E values. Road transport uses vehicles that are commonly available, and hence actually contribute little to E_n values for which n is close to 1. A staffed petrol station cannot, however, be operated without staff present; this incurs a vulnerability of nonavailability because staff facilities (sewage disposal, provision of water, and lighting) are unavailable. Staff facilities are a major contribution to the total exposure that the complete system incurs for the end user.

D. Targeted First Aid

Acute medical issues can arise at any time, and for many examples, simple actions make the difference between life and death. The specific service in this example is the correct application of first aid for treating acute choking, i.e., the foreign body blockage of the airway. The remedy for acute choking is the "Heimlich maneuver" [14]. Assuming that the end user does not have significant first-aid training, the user is reliant on a technological approach to get the "service," i.e., the diagnosis and treatment information required. The diagnosis of choking is not difficult though it may not be trivial either. The Heimlich maneuver is simple to perform, but is it not intuitively obvious. The first-aid provider must, therefore, communicate symptoms and undertake the action that is described by a remote expert (human or machine).

The provision of the first-aid advice depends critically on the availability of a knowledge base that has the capability to understand symptoms, and to identify and describe recommended actions in a form and timeliness to allow a remedy. The representative example system uses an Internet-connected PC to access a remote diagnostic and advisory system. The local PC and last-mile communications contribute exposure as does the remote diagnostic and advisory system. The Internet communications subsystems (up to and including peering points) are as described in the work information example, however, since a national diagnostic and advisory system is assumed, the undersea cables make no contribution to exposure. Because the example proposes an Internet-mediated communication, the analysis shows that the end user is vulnerable to the nonavailability of the Internet. The first aider is also vulnerable to a failure of the consultant system, whether human or artificial, which generates the diagnosis and recommends treatment.

E. Perishable Food

Many staple foods including fresh milk, have short shelf lives and are too bulky to allow significant storage. The capability to acquire supplies on a regular basis is essential to an urban dweller's lifestyle. The service for this example, is the supply of fresh milk. The example considers the availability of a consumer container of acceptable quality milk, in the refrigerator of the user's apartment. In this context, the service equates to a product in the user's refrigerator, and contributors to exposure include the apartment power supply and access to the apartment, user storage, user transport, retail transaction processing, the retailer system, retailer staff facilities, and bulk

transport to the retail facility, raw milk processing, and the raw milk collection system. This example must consider the aggregation, processing, transport, and retailing of milk. Since a large number of farms produce the raw material and a large number of tankers are capable of farm-collection, it is reasonable to consider that example scope beyond the processing plant's reception area is adequately duplicated. An EFTPOS transaction, as previously described, is assumed to be required at the retail outlet. Specifically, this analysis shows that the end user is vulnerable to the failure of the financial transaction system (e.g., EFTPOS) and that in turn is vulnerable to failures of the Internet communication system. For a short shelf-life product, dependence on a single centralized processing facility incurs particular vulnerability to the end user. Transport systems have high levels of design redundancy and therefore incur minimal vulnerability. In addition to the vulnerabilities associated with the transactional facility, the retail facility's dependence on staff, and hence staff facilities, incurs significant vulnerabilities for the end user.

F. Essential Specific Medicine

For many conditions including asthma, a supply of medicine allows a person to function normally, and conversely a lack of medication will require hospitalization and cessation of normal lifestyle. The service, in this case, is the supply of an essential medicine. The medicine selected is Salbutamol sulphate, marketed as "Ventolin." The service will be considered to have been delivered when a fully charged Ventolin metered-dose-inhaler (MDI) is acquired by a user. The user acquires a workable MDI using a financial transaction and prescribing permission (an EFTPOS transaction is assumed). MDI filling, packaging, and distribution systems create the MDI using a filling with an active ingredient formulation, pressurization with propellant, assembly of the metering valve and sealing of the completed unit, testing and packaging, and shipping and distribution chains. The manufacture and filling of MDI containers have the following components: the container, metering valve, and actuator (plastic mouthpiece/holder). The container is manufactured by taking an aluminum sheet and using an electrohydraulic deep-drawing press to create the container. The metering valve is created using the perforated actuation tube that releases the dose when depressed and allows loading of another dose of propellant plus the active ingredient when released from depression.

This would normally be formed using an electrically operated CNC lathe, from an aluminum or plastic tube stock. The metered-dose chamber is formed by a deep-drawing operation. The container and cap are each formed by a common electrically operated pressure-injection process using a thermoplastic. The metering valve is assembled using common semi-automated processes. The MDI active ingredient (Salbutamol sulphate) is synthesized [15] from raw feedstock materials that are available from a large number of sources. It is tested, diluted and distributed for the filling operations. The analysis shows that the end user is vulnerable to the availability of the financial transaction system, which in turn is vulnerable to the availability of the Internet system. As noted previously, the transport system has high levels of design redundancy and so incurs little vulnerability. The manufacture of the MDI canister also incurs limited vulnerability, but the local filling operations do incur notable vulnerability and the centralized synthesis of the active ingredient also incurs significant vulnerability.

IV. Results

A. Current Technological Vulnerabilities and Trends

The dependence of urban dwellers upon technological systems has been noted, and we have shown that the number and nature of weaknesses in any such system is a measure of the vulnerability imposed on each end user. Examination of the example studies have shown that technological systems' contribution to end-user vulnerability is considerable, and can be classified within a small number of categories that each have distinctive aspects. The distinctive categories of exposure suggest distinctive but generalizable approaches to reductions in exposure. As well as currently practical options, the analysis has also allowed the identification of technological capabilities such as power storage that are not yet feasible but would contribute significantly to exposure reduction.

Since the first industrial revolution, urban dwellers' dependence upon, and hence vulnerability to technological systems have steadily increased. These systems have been historically capable of supplying basic needs, however, in response to the growth of urban populations, these essential technological systems have grown in scale, complexity, and interconnectedness. Since the degree of urbanization is projected to increase, as is the total population, these trends are likely to cause further increases in the exposure of the technological systems serving urban dwellers. Both the examples, and the projected trends add quantitative evidence to support intuitively held concerns for personal security at present and in a projected future.

B. Exposure Categories

The contributors to each technological system's exposure may be grouped into a small number of categories and the generalizable features of each category are described in detail. For each category of exposure, this article develops generalized approaches for reducing the exposure of existing or planned system and hence the vulnerability imposed upon the end user. Results from these analyses will be shown to demonstrate that the theory of exposure can be used to develop broadly applicable and practical approaches to the reduction of end-user vulnerability, and also suggests the feasibility of less exposed technological systems. An analysis of the systems' vulnerabilities, using the principles of qualitative classification [16] confirms that the exposure points/vulnerabilities can be grouped in a small number of categories. This analysis is significant, since without a categorization, the numbers of possible solutions would be unbounded; with a useful categorization a generalization of results is possible.

1) Initial Resource Availability: All technological systems producing goods and services for users ultimately depend upon

raw materials and viable environmental conditions. Where raw materials cease to become available, or environmental conditions change permanently, services to users will inevitably fail. Raw material supplies and acceptable environmental conditions must, therefore, be identified [17] as sources of exposure and hence vulnerability to users. Many authors, of whom [18] is but one example, have identified major environmental failure as an "existential risk," potentially affecting the totality of life on Earth [18], extending to a scope much wider than that which is addressed in this article.

2) Single Points of Failure: All single points-of-failure (SPOF) contribute to E_1 values and so make a primary contribution to the user's vulnerability. We find three subcategories of SPOF. The first is where delivery of services to users involves some processes immediately adjacent to the user, known as "last-mile" services in the telecommunications field. The second subcategory of SPOF is illustrated by considering a small rural town whose EFTPOS, landline phone service, cell-phone service, and Internet connection have all been progressively migrated to data services, carried by a single fiber-optic cable and thus have inadvertently created an SPOF. The third is where a particular failure will inevitably cause failure of other components that are not functionally connected—a cascading failure. The last-mile subcategory of SPOF, justifies always including the final delivery to users within the consideration of technological systems: the analysis of specific technological systems' exposure allows the identification of inadvertent SPOF's, and a rigorous analysis of subsystem processes should identify potentials for cascading failures.

3) Complex Unit Operations: We refer to the descriptor "complex" as a characteristic of a process whose internal operation is practically unknowable to the user and cannot realistically be repaired by the user. In examples, such as the work information and the first aid examples, personal computers, routers, and related equipment are used. Users will not have deep insight into the operation of the CPU, memory, or interface circuitry of their PC and fewer still would have significant capability to diagnose faults and carry out repairs. It is also possible to consider situations where a critical application has been compiled from an outdated programming language and runs on a computer for which no spare hardware is available. Another example might consider critical information held on a very old storage medium [19]. These examples illustrate three categories of complex processes: in the first case, while the inner workings of a PC may be exceedingly complex, the format of incoming data (TCP/IP packets) and protocols (WWW, e-mail, etc.) are in the public domain and so it is not only possible but also practical for alternative machines to offer the same services. In the second case, assuming the functional specifications of the application processes are known, the application can be recorded (and fully documented) using a language for which larger numbers of maintenance programmers exist, and on a more common platform. The third case of data encoded on old storage medium, illustrates a subcategory where the internal details of the storage are proprietary (not in public domain), alternative equipment is unavailable, and creation of replica equipment for reading the data is probably impractical, leading some authors [20] to express fears of a "digital dark age."

4) Lack of Buffering: For the Salbutamol example, it is both possible and practical to provide buffer stocks of active ingredients, dilutants, and MDI components at various points in the process. Perishable food supplies and sewage evacuation are examples where buffering of streams is possible, though with perhaps limited practicality. All processes involving uses of 230VAC or 110VAC will fail immediately if the power supply fails; this is a case where the practical and economic lack of a technological capacity to store buffer quantities of a stream (i.e., electrical energy) is not currently possible and such supplies always contribute to exposure.

5) Highly Centralized Processes: The evacuation and treatment of sewage requires a network of pipes and pumps to collect sewage and deliver it to the treatment station. This is an example of a centralized system that is large but technologically simple. Other examples of large centralized systems include financial transaction systems [21], and the international data transmission systems of undersea fiber-optic cables. These highly centralized systems offer services upon which the user depends, yet for which the user has few alternative sources. Such systems tend to be monopolies and are commonly controlled by entities that have little if any obligation to provide service or to negotiate terms acceptable to individual users. These characteristics of highly centralized systems cause significant contributions to the user's vulnerability.

6) Contributory Systems: Whenever a system is made dependent upon another, the contributory system's exposures are reflected in the total exposure to the user. In the first aid example, the user of an Internet diagnostic and advisory approach causes the full exposure values of the Internet, including local PC and last-mile services, to be contributed to the end-user's vulnerability. Payments that are only possible via online banking or via EFTPOS facilities similarly accrue the larger exposure values of those systems. Some subcategories can be distinguished; the use of the Internet in the work information example is difficult to avoid, however, cash payments are technically feasible for local services and EFTPOS is not technically necessary. For the sewage treatment example, remote operation of pumps may be efficient, but it is quite feasible to include "local/manual" control provisions allowing operator intervention if the remote control is unavailable or undesirable. For the first aid example, a paper first-aid manual is eminently practical, as is the local electronic storage of reference information.

7) Practical Unavailability: We may consider the hypothetical case where a user wishes to communicate sensitive information, but only has access to one data transmission facility that is known to be under surveillance. Although technically operational, the inevitable absence of privacy associated with the data transmission facility, in this hypothetical case, has made the facility practically unavailable. For technological systems that are highly centralized and near-monopoly, practical unavailability is a significant possibility.

Table I identifies examples to which each exposure category is particularly applicable.

TABLE I
CATEGORIES OF EXPOSURE AND EXAMPLE APPLICABILITY

Category	Significant example applicability
Initial resource availability	Fuel supply. Food. Fuel.
Single points of failure (SPOF)	Fuel. First-aid. Sewage.
Complex unit operations	Work info. First-aid. Fuel.
Lack of buffering	Medicine. Sewage. Fuel Food.
Highly centralised processes	Work. First-aid, All financial transaction. Sewage.
Large contributory systems	Fuel. First-aid. Work info.
Practical availability	Work info. All financial transactions.

C. Trends of Exposure Level and Nature

An inspection of the examples allows reflection on the historical processes that have led to the current technological approaches, and also allows speculation on the possible future directions for the supply of these and similar goods and services. The technological systems described have arrived at their current configurations after progressive development arising from a range of drivers, rather than a single design step. It is important to describe and distinguish these drivers, since any realistic proposal for change needs to address them.

Several drivers can be discerned, and more than one driver may contribute to the current approach to a particular technological system.

1) Minimum Capital Investment: For subsystems, such as an undersea fiber-optic cable, or a microprocessor fabrication plant, it could be argued that there is a minimum level of capital investment required to implement some moderately current capability. That level is likely to be vastly above what can be considered by an individual, and hence will only be undertaken by a corporate that envisages a competitive return on investment (ROI).

2) Compliance/Regulatory Requirements: Sewage treatment and the provision of potable water have been one of the most tangible contributions of professional engineering to the average lifespan of humanity. Both have evolved to the point where their outputs (treated waste in one case, drinking water in the other) are obliged to comply with internationally accepted quality standards.

3) Economies of Scale: Economies of scale are evident in many cases. At a large-city scale, a cogeneration system using methane from the digestion of sewage is often found to be economically viable, however, chemical and process engineers have found that plant capital and operating costs commonly rise at a rate equivalent to only about a 0.66 exponent of the scale ratio [22] and so a household-scale version faces significant hurdles. The scaling exponent for capital cost does, however, vary significantly for differing technologies, and for photovoltaic (PV) technologies small scales do not necessarily face the same hurdles.

4) Necessity for Standardization and Interoperability: We can observe cases in which designers of technological systems have, for a range of reasons not necessarily focused on end-user vulnerability, have acted to achieve a level of standardization and interoperability. Prominent examples are varied and include the standardization of motor fuel (petrol and diesel) specifications, agreement on shipping container dimensions and fittings [23], TCP/IP protocols [24] for Internet data, and to a lesser extent, agreement on voltage and frequency specifications for electric power. The agreement (with the notable exception of one major country) upon such fundamental issues as standard units of measurement (SI), and chemical symbols and written characters (ASCII) are also notable. Even the limited standardization of such mundane items as cell-phone charger plugs (micro-USB) have contributed significantly to a decrease in end-user vulnerability.

5) Specific Need for Breadth of Cover: Cases can be identified where the breadth of applicability is essential: in a global marketplace the capability to complete a financial transaction regardless of geography requires an acceptance of a unit of value, and an assurance that a vendor (wherever located) can actual gain useful credit from a remote purchaser. Such requirements can be expressed in quite broad terms, but irrevocable transfer of value does imply a need for the breadth of cover. Information search systems (major Internet search engines) acquire value according to the breadth of resources that are indexed. Reviewing the historical issues that have led to current levels of exposure, it is possible to extrapolate these trends and examine some factors that would either advance or retard them.

6) Complex Proprietary Systems: Competitive pressures will create tensions in large companies (e.g., manufacturers of cellphones, PCs, and highly computerized cars) to use increasingly complex, undocumented systems. The potential consequences particularly for data storage, have been noted by authors such as [25].

7) Depletion of Natural Resources: Increased dependence on rare resources is an issue affects items as diverse as genuine vanilla flavor, coffee beans, advanced CPU and RAM chips and rare-Earth metals [26]. Trends involving the depletion of natural resources have been extensively reported elsewhere, fossil fuels are a particularly significant example [27].

8) Centralization Due to Regulatory Pressures: A trend to increase regulation of activities that affect others can be discerned and is arguably an inevitable result of higher density living. The disposal of rubbish in a town rubbish dump has become unacceptable and caused a transition to large, carefully designed, and remote dumps. Small-scale wood-burning appliances have come to be prohibited in many locations.

9) Decreased Buffering Stocks: All stockpiles have capital value, and the cost of capital has driven an increasing dependence on just-in-time (JIT) supply chains and corresponding lack of buffer stocks. Examples include international foods, construction steel, and transport fuel.

10) Increase Contributory System Exposure Due to Incorporation of Features: A trend to include requirements for Internet connectivity in many systems is observed. This trend adds large exposure associated with the contributory system (Internet). Similarly, the trend to discourage the use of cash in favor of electronic transactions inevitably adds

enormous contributory system exposure to any case where a financial transaction is required.

11) Practical Accessibility Issues: Commercial service providers including Internet search and social media services and also financial service institutions and public services, are increasingly able to mandate terms and conditions that are unacceptable to individuals. Where alternative services are not available (i.e., no technological alternative exists), such conditions make the service itself "practically unavailable" to a user.

12) Increase Local Capability: We must also note that some trends, including computing, 3-D printing, and solar PV systems represent trends toward decreased exposure, by bringing capabilities close to the point of need.

V. Discussion and Conclusion

A. Trends

For the specific grouping studied in this article, most trends are toward increased exposure, inviting speculation that without change, urban populations will approach a situation of such high exposure that failures are almost inevitable. These trends also invite speculation on what a low-exposure society would look like, the possible pathways to such a state, and the approaches available to decision makers that would enable/facilitate exposure reductions.

B. Reduced Exposure: Principles and Approaches

The analysis of technological system vulnerabilities must be set alongside the observation that a large and increasing percentage of the population of Earth still seek levels of security for their life-necessities, and hold intuitively perceived concerns related to their vulnerability, while valuing the goods and services to which they have access. A trend toward higher exposure values and the associated loss of personal security for such a large and rising percentage of the world's population, is a prospect that will not appeal to the human values of the urban-dwelling portion of that population.

1) Present Goal: The demonstrated exposures and their trends are neither short-term nor narrow in scope, and so the proposed approaches to exposure reduction are generalizable and applicable to a broad range of issues. By defining exposure in a way that allows quantitative comparison of alternative solutions, we can realistically hope to minimize the solutions breed new problems paradox [1].

2) Future Goals: In the future, we might consider the lowest level of exposure that could be accepted and reasonably aspired-to, assuming a functionality and level of sophistication similar to present. Others [28] have previously debated the level of risk that society is prepared to take, and this issue has some similarities to the "accept" principle of risk management [29]. A robust debate on the level of acceptable exposure seems equally significant and more likely to generate long term solutions in the future.

Yet further in the future, we might ask, for a defined level of acceptable exposure, "What is the smallest societal unit-size that can achieve this?" Isaac [30] postulated a fictional and tiny population of human beings, whose every need was supplied by a technological system (intelligent robots), and thus a society in whose citizens were effectively insulated from any significant technological vulnerability. His novels thus contemplated a society in which personal von-Neumann machines [31] reduced individual exposure to a very low figure. As the discussion of the possibility of a self-sustaining Mars colony continues, this question assumes very practical significance and appears to be a topic worthy of significant future work. This article has focused on the identification of exposure/vulnerability and the simple feasibility of reductions: the prioritization of exposure reduction efforts and the managerial/governance and social issues associated with significant change have not been considered within the scope of this article, but would seem to justify future research.

3) Principles: Common elements of the management of risk [29] include avoidance, reduction, sharing, or retention: the reduction of a system's exposure primarily relates to the "avoidance" (removing loci of weakness) aspect, however, reducing all high exposure values (e.g., E_1 and E_2) to zero does have similarities to the concept of risk sharing. We propose that the analysis of exposure has generated significant insights in addition to those which could have been obtained by risk management approaches, and these insights, in turn, generate principles for decreased vulnerability. Table II describes generalized approaches to each of the categories of exposure. In addition to the general principles set out in Table II, several very specific issues may be noted.

Exposure Due to Lack of Standardization of Information Storage (Complex Unit Operation): A reduced exposure option for the first aid example is the local storage of information. Further examination of that alternative shows that while character coding is standardized [32] the representation of information on nonvolatile storage still contributes significant exposure at present. The drive to higher data densities on hard-disk platters and compression algorithms represents a consumer boon, but a source of exposure. Others [20] have noted this issue and have foreseen a digital dark ages as a possible outcome. While no standardized long-life format has been agreed, we may note that technologies, such as that proposed for the "Rosetta disk" [33] and the "5-D data storage" medium proposed by the University of Southampton [34] are possible moves toward this goal.

Innovations With Potential to Decrease Highly Centralized Operations: Innovations, such as 3-D printing [30], 5-axis milling [36], "lab on a chip" [37], and general-purpose synthesis equipment [38], all represent technologies that have the potential to decentralize some capabilities. A domestic 3-D printer capable of creating a motor vehicle part has markedly reduced the exposure associated with a remote factory and international distribution system. The use of cryptocurrencies based on blockchain technology [39] and gold bullion are examples of decentralizing technologies. Technologies such as the use of macro-algae [40], which can produce crude liquid fuel on a scale only nominally larger than the scale required by an individual apartment

TABLE II
OPTIONS FOR REDUCTION OF EXPOSURE

Category of exposure	General approach to reduced exposure
Initial resource availability	Public awareness of this exposure. Conservation of scarce resources. Development of alternative sources.
Single points of failure (SPOF)	Incorporation of design redundancy, with specific aim of reducing E_1 (and possibly E_2) to 0.
Complex unit operations	Public standards for input/outputs allows alternatives to emerge. For many complex unit operations, buffer stocks of the complex subsystems themselves is practical, and reduces exposure in the operational and maintenance timeframes. Secure escrow of design information would reduce specific examples of complex unit operation exposure.
Lack of buffering	For all high value, long-life goods the maintenance of buffer stocks is a practical measure. Buffering should decrease the ratio between "mean time to restore supply" and "mean time to exhaust stock".
Highly centralised processes	Ensure non-centralised alternatives remain in operation. Provide standard specifications for process outputs to allow local duplication of services. Specific technologies that offer decentralising functionality.
Large contributory systems	Avoid system configurations in which local operations are dependent upon contributory systems. Design-in alternatives to mandatory contributory systems, which will reduce exposure at E_1 levels.
Practical availability	Regulatory approaches to ensure service availability and preclude unreasonable access conditions. Consumer pressure to fund alternative access options, and to fund access on consumer's terms.

dweller, are also potential routes to decreases in exposure for goods that are currently produced in highly centralized systems.

Design Options to Avoid High Exposure From Contributory Systems: Large subsystems may introduce very large numbers of contributory exposure points. For example, a design that includes an Internet connection to an internal cardiac defibrillator (ICD) inevitably creates an enormous contributory exposure [7], since every Internet user and every Internet component and protocol can potentially affect the operation of the ICD. For services, efforts to decrease contributory exposure levels press us toward a more decentralized technological model. For goods (as opposed to services), centralized systems also inevitably introduce significant contributory exposure levels, which may, however, be mitigated by combinations of buffering and standardization (allowing multiple alternative suppliers). No communication technology with the capability of the Internet exists at present, yet an Internet connection represents a huge contributory exposure for any connected system.

Avoidance of Exposure to Complex Unit Operations: Although the detailed design of a modern CPU chip is unlikely to ever be public and standardized, the combined chipset/board, operating system, and application can be treated as a unit provided only that the input and output formats are standardized. Applying the general principle of public I/O specifications, it may be noted that an open document file (ODF) [41] has a standardized format and can be viewed and edited by either a desktop PC running Windows on an Intel chipset, or by Libreoffice running under Linux on a Raspberry Pi, or common applications for Android, and thus the exposure to the complex unit operation is reduced.

Avoidance of Practical Unavailability: Electronic financial transactions and Internet access carry a high possibility of "practical unavailability," associated with their centralized nature and the range of systems dependent upon them. Retaining the option of cash transactions/payments and enabling the use of cryptocurrencies reduces the exposure due to the practical unavailability for centralized electronic financial transactions. Mandating privacy and accessibility, and ensuring access to encryption will reduce exposure to practical unavailability of Internet use.

C. Exposure Reduction Options

In response to the high and increasing levels of technological exposure, this article has not only classified the nature of current and projected technological exposure but also has proposed generalizable approaches to reduction. The economic practicality of exposure reductions is somewhat dependent on the value assigned to security. However, many approaches are practical in view of the economic costs and capabilities of the individuals affected.

Bringing a technologically feasible project to fruition requires practical approaches to social and political requirements. It is not within the scope of this article to develop a comprehensive project plan for a reduced-exposure society, but without evidence of feasibility any recommendations become mere curiosities. For some exposure reduction opportunities, barriers to uptake are minimal: there is already widespread uptake of household PV capabilities, and the availability of improved battery and control systems are collectively enabling reduced dependence on ac power distribution. Cellular phone and WiFi uptake are similarly enabling change to the last-mile communications landlines. For some other exposure reduction options, barriers to change would require little more than a change in the perception of values: large Internet player providers of social media services rely on business models that sell user data to retailers and data analytics companies. A revision of the value assigned to privacy could very simply invert this model to one where users' prefer to pay a small fee for social media services, and regain control of their privacy.

The topic addressed in this article faces an additional barrier that is neither technological nor economic in nature. A lack of precise and accepted definitions of such terms as risk, "vulnerability," "exposure," "resilience," "robustness," etc., hampers the clarification of issues and progress toward solutions of them. For common terms in this field, definitions that are explicit and nonoverlapping have been proposed [42] and a set of clear and nonoverlapping definitions will assist in clarifying discussion of this field.

D. Feasibility

This article describes a set of examples that illustrate several categories of exposure, particularly applied to individuals. By considering the categories of exposure, generalizable approaches to reducing exposure have been developed, as well as some specific applications to the examples. The technological feasibility of the general approaches to each category of exposure will now be considered, without restriction to the scope of the specific examples. Of the specific exemplar approaches to reducing exposure, we note that many are already technically mature and require only to clear economic hurdles and achieve either personal or organizational decisions to implement. Other technologies, such as the 3-D printing (with engineering materials), small-scale creation of sophisticated materials, general-purpose chemical synthesis exist with relatively low technological maturity [43] and in many cases limited scope. The maturity of these technologies are however advancing rapidly, and it is reasonable to consider their long term effect on the individual's vulnerability to technological systems. Even when specific technological capabilities are not currently available, it is useful to consider whether there are fundamental issues that would limit reasonable expectations that the capability will be achieved.

In the absence of fundamental difficulties, one might simply ask what drivers would be required in order to provide a reasonable expectation of successful development. We may note, as an example, that a group of Australian high-school students demonstrated the ability to synthesize Daraprim [44]. The specific examples analyzed in this article have also revealed a number of causes of exposure that can be categorized as current technological gaps; this identification is considered inherently useful. When considering technological capability gaps, it seems important to determine whether these current gaps are the result of some fundamental limitation or whether there is evidence that they are intractable. Perhaps the most significant capability gap at present is that while battery systems capable of storing significant amounts of electrical energy have been assembled, there is currently no commercially viable technology that can store MegaWatt-hours (MWh) of electrical energy in a practical and economical way, and while no fundamental issues appear to make such a goal impossible, neither economic drivers, nor R&D efforts over many years, have commercialized this capability. It does seem likely that Shannon's law and square-law issues will limit free-field communication rates [45], however, there does not appear to be any fundamental barrier to a low-rate decentralized communication system.

Mass production philosophy has commonly assumed that a piece of machinery (e.g., equipment to machine an engine block for a vehicle motor) is expensive and can do only one thing, so the machinery must do that one thing very many times to justify its cost. This basic philosophy is challenged by an inexpensive piece of machinery that can do a wide variety of tasks. Noting that technologies such as 3-D printing are maturing rapidly, it is reasonable to speculate on the effect of an affordable "backyard" technology that can practically replace any vehicle part or household component. The possibility that a general-purpose machine can recreate and assemble all parts required for a duplicate of itself is a trivial additional step, yet would represent a true, long-term decentralization and a long-term decrease in user vulnerability to technological systems. In such a decentralized manufacture scenario, design information would become the most important traded item. Current patent legislation was designed to balance the reasonable right of an inventor to profit from their invention, and the need for capabilities to be made generally available and to form the basis for further development: this balance would become even more significant in such a case. For some technologies (communications satellite, undersea fiber-optic cable) it is perhaps less likely that small-scale, low-capital replacement technologies will arrive quickly, and we might consider how capital for such capabilities could be assembled without incurring problems of general access.

E. Toward More Robust Future

It has been proposed [46] that members of society ultimately weigh the value against the total cost of societal membership, and when the cost outweighs the value a possibility of disruption and collapse exist. This article has presented analyses showing that technological systems have significant exposure, which is correlated with the vulnerability of individuals who depend on those systems' outputs. Technological systems have certainly offered members of society significant value, yet perceptions of vulnerability, concerns over privacy, and related concerns contribute large costs.

The societal significance of this issue is high: human values of security, independence and autonomy must be retained as science and technology advance and although the capabilities offered by technological systems are huge, this article shows that under present trends the individual vulnerability "costs" are rising apiece and have potential to overwhelm the capabilities. This article has focused on technological aspects and while much technological development is certainly needed, even larger sociological development is required to address the corporate/structural drivers that generate increased exposure/vulnerability. Nevertheless, both the issue- and trend-clarification, and the technical feasibility of retaining capabilities while reducing the individual vulnerabilities/costs, is proposed to be useful. We might indeed ask where such options could lead us? Such scenarios could occur in a Moon or Mars colony, and have been explored by science fiction authors such as Isaac Asimov. Specific technologies including 3-D printing, 5-axis milling, sophisticated small-scale chemical synthesis, lab-on-a-chip, and trust-free distributed concepts, such as the blockchain, reduce contributions to technological exposure, and we propose that the application of a theory of exposure has focused attention on the significance of such technologies. Simple measures such as retention of cash/bullion options for financial transactions also offer major reductions in exposure and should be adopted for that reason. The avoidance of practical unavailability is amenable to regulatory enforcement of citizens' access rights, privacy rights, and such topical issues as "right to repair." The analysis of exposure has also allowed the identification of specific

capabilities (power storage) that are yet to mature and has clarified some societal and commercial barriers. The analysis of weaknesses, and the corresponding highlight of technological solutions presents a practical vision of a technologically sophisticated society with significant technological exposure only to environmental factors.

ACKNOWLEDGMENT

This article draws on material presented in a thesis titled "Identifying and reducing technological contributions to end-user vulnerability," presented by L. J. Robertson, in fulfilment of the requirements for the award of the Degree of Doctor of Philosophy at the University of Wollongong.

REFERENCES

[1] P. M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York, NY, USA: Doubleday, 1990, ch. 4. Accessed: Sep. 2017. [Online]. Available: http://leeds-faculty.colorado.edu/larsenk/learnorg/senge.html

[2] M. S. Swaminathan, "Obituary: Norman E. Borlaug (1914–2009) plant scientist who transformed global food production," *Nature*, vol. 461, no. 7266, p. 894, 2009.

[3] R. N. Webb, "James Watt: Inventor of a steam engine," Watts Ltd., North Andover, MA, USA, 1972.

[4] R. Batchelor, *Henry Ford, Mass Production, Modernism, and Design*. Manchester, U.K.: Manchester Univ. Press, 1994.

[5] A. Ledwoch, A. Brintrup, J. Mehnen, and A. Tiwari, "Systemic risk assessment in complex supply networks," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1826–1837, Jun. 2018, doi: 10.1109/JSYST.2016.2596999.

[6] Y. Y. Haimes and P. Jiang, "Leontief based model of risk in complex interconnected infrastructures," *J. Infrastruct. Syst.*, vol. 7, no. 1, pp. 1–12, 2001.

[7] L. J. Robertson and A. Munoz, "System configuration contributions to vulnerability: Applications to connected personal devices," *IEEE Technol. Soc. Mag.*, vol. 36, no. 1, pp. 52–57, Mar. 2017.

[8] C. Perrow, *Normal Accidents: Living With High-Risk Technologies*. New York, NY, USA: Basic Books, 1984.

[9] O. D. Cardona *et al.*, "Determinants of risk: Exposure and vulnerability," in *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC)*, C. B. Field *et al.*, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2012, pp. 65–108.

[10] (2009). *The Population Reference Bureau*. Accessed: Sep. 19, 2017. [Online]. Available: http://www.prb.org/

[11] L. J. Robertson "Identifying and reducing technological contributions to end-user vulnerability," Ph.D. dissertation, School Comput. Inf. Technol., Faculty Eng. Inf. Sci., Univ. Wollongong, Dec. 2017.

[12] L. J. Robertson, "From societal fragility to sustainable robustness: Some tentative technology trajectories," *Technol. Soc.*, vol. 32, no. 4, pp. 342–351, 2010.

[13] A. H. Maslow, "A theory of human motivation," *Psychol. Rev.*, vol. 50, no. 4, pp. 370–396, 1943.

[14] *St. John Guide to First Aid in a Choking Emergency*. Accessed: Feb. 26, 2017. [Online]. Available: http://www.stjohn.org.nz/First-Aid/First-Aid-Library/Choking/

[15] *ChemWiki Synthesis of Salbutamol*, Imperial College, London, U.K. 2016. Accessed: Feb. 26, 2017. [Online]. Available: http://www.ch.ic.ac.uk/local/projects/j_hettich/salbutamol/noframes/nfsynthesis.htm

[16] K. D. Bailey, *Typologies and Taxonomies: An Introduction to Classification Techniques*. Thousand Oaks, CA, USA: SAGE, 1994.

[17] J. Diamond, *Collapse: How Societies Choose to Fail or Succeed*. New York, NY, USA: Penguin Books, 2005.

[18] H.-Y. Liu, K. C. Lauta, and M. M. Maas, "Governing boring apocalypses: A new typology of existential vulnerabilities and exposures for existential risk research," *Futures*, vol. 102, pp. 6–19, Sep. 2018.

[19] E. R. Teja, *The Designer's Guide to Disk Drives*. Reston, VA, USA: Reston, 1985.

[20] V. Cerf, "Digital vellum," presented at the AAAS Annu. Meeting, Feb. 2015. Accessed: Sep. 2017. [Online]. Available: https://aaas.confex.com/aaas/2015/webprogram/Paper14064.html

[21] D. O'Mahony, M. Peirce, and H. Te Wari, *Electronic Payment Systems*. Boston, MA, USA: Artech House, 1997.

[22] A. M. Gerrard, Ed., *Guide to Capital Cost Estimating*. Rugby, U.K.: IChemE, 2000.

[23] M. Levinson. (2006). *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*. Accessed: Sep. 19, 2017. [Online]. Available: http://press.princeton.edu/chapters/s9383.html

[24] R. Braden, Ed. (Oct. 1989). *Network Working Group, Internet Engineering Task Force. Request for Comments: 1122*. Accessed: Sep. 19, 2017. [Online]. Available: https://tools.ietf.org/html/rfc1122

[25] D. P. Bergeron, *Dark Ages II: When the Digital Data Die*. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.

[26] S. Massari and M. Ruberti, "Rare Earth elements as critical raw materials: Focus on international markets and future strategies," *Resources Policy*, vol. 38, no. 1, pp. 36–43, Mar. 2013.

[27] R. Heinberg, *Snake Oil: How Fracking's False Promise of Plenty Imperils Our Future*. West Hoathly, U.K.: Clairview Books, Mar. 2014.

[28] T. Aven, "On some recent definitions and analysis frameworks for risk, vulnerability, and resilience," *Risk Anal.*, vol. 31, no. 4, pp. 515–522, 2011.

[29] O. E. Ogunsanmi, O. A. Salako, and O. M. Ajayi, "Risk classification model for design and build projects," *J. Eng. Project Product. Manag.*, vol. 1, no. 1, p. 46, 2011. [Online]. Available: https://search.proquest.com/openview/bb4221a011291cb0e86bf1967c61631f/1?pq-origsite=gscholar&cbl=706377Sept2017>

[30] A. Isaac, *The Robots of Dawn (Robot #3)*. New York, NY, USA: Bantam Books, Mar. 1994.

[31] R. A. Freitas and R. C. Merkle, *Kinematic Self-Replicating Machines*. Georgetown, TX, USA: Landes Biosci., 2004.

[32] C. E. Mackenzie, *Coded Character Sets, History and Development (PDF)* (The Systems Programming Series). Reading, MA, USA: Addison-Wesley Develop. Press, 1980. Accessed: Sep. 2017. [Online]. Available: http://www.evertype.com/standards/iso10646/pdf/cwa13873.pdf

[33] *Rosetta Disk*, Longnow Found., San Francisco, CA, USA. Accessed: Sep. 19, 2017. [Online]. Available: http://rosettaproject.org/disk/concept/

[34] *Eternal 5D Data Storage Could Record the History of Humankind*, Univ. Southampton, Southampton, U.K., 2017. Accessed: Feb. 26, 2017. [Online]. Available: http://www.southampton.ac.uk/news/2016/02/5d-data-storage-update.page

[35] G. Banning, "3D printing: New economic paradigms and strategic shifts," *Global Policy*, vol. 5, no. 1, pp. 70–75, 2014.

[36] A. Álvarez, L. N. L. de Lacalle, A. Olaiz, and A. Rivero, "Large spiral bevel gears on universal 5-axis milling machines: A complete process," *Procedia Eng.*, vol. 132, pp. 397–404, Dec. 2015.

[37] *Lab on a Chip*, Roy. Soc. Chem., London, U.K. Accessed: Feb. 26, 2017. [Online]. Available: http://www.rsc.org/journals-books-databases/about-journals/lab-on-a-chip

[38] K. E. Drexler, "Molecular engineering: An approach to the development of general capabilities for molecular manipulation," *Proc. Nat. Acad. Sci. USA*, vol. 78, no. 9, pp. 5275–5278, 1981. Accessed: Sep. 6, 2016, doi: 10.1073/pnas.78.9.5275.

[39] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc., Sebastopol, CA, USA, Jan. 2015.

[40] H. Chen, D. Zhou, G. Luo, S. Zhang, and J. Chen, "Macroalgae for biofuels production: Progress and perspectives," *Renew. Sustain. Energy Rev.*, vol. 47, pp. 427–437, Jul. 2015.

[41] *Information Technology—Open Document Format for Office Applications (OpenDocument) V1.2—Part 1: OpenDocument Schema*, ISO/IEC Standard 26300-1:2015, 2015.

[42] L. Robertson, A. M. Aneiros, and K. Michael, "A theory of exposure: Measuring technology system end user vulnerabilities," in *Proc. IEEE Int. Symp. Technol. Soc. (ISTAS)*, Sydney, NSW, Australia, 2017, pp. 1–10.

[43] J. C. Mankins, "NASA technological maturity. Technology readiness assessments: A retrospective," *Acta Astronautica*, vol. 65, nos. 9–10, pp. 1216–1223, Nov./Dec. 2009.

[44] M. R. Binns, *Open Source Malaria Daraprim Synthesis*. Accessed: Sep. 19, 2017. [Online]. Available: http://malaria.ourexperiment.org/daraprim_synthesis

[45] C. E. Shannon, "Communication in the presence of noise," *Proc. Inst. Radio Eng.*, vol. 37, no. 1, pp. 10–21, 1949.

[46] J. A. Tainter, *The Collapse of Complex Societies*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

Lindsay J. Robertson received the Bachelor of Engineering degree in mechanical engineering design and thermal systems from Canterbury University, Christchurch, New Zealand, in 1976, the Master of Technology degree (First Class Hons.) from Massey University, Palmerston North, New Zealand, in 1990, and the Ph.D. degree from the University of Wollongong, Wollongong, NSW, Australia, in 2017 on the theme of technological risk, exposure, and resilience.

From 1976 to 1987, he held positions with New Zealand Government, Wellington, New Zealand. From 1990 to 2007, he worked with Fonterra (and NZ Dairy) Research Centre, Palmerston North, and a Principal Engineer with Parsons Brinckerhoff, New York, NY, USA, from 2007 to 2016. He was with Fonterra Research and Development Centre, Palmerston North.

Dr. Robertson was the Editor-in-Chief of *IPENZ Transactions* from 2002 to 2016. He has been a fellow within the Institution of Professional Engineers, New Zealand, since 1999 and also the Institution of Mechanical Engineers, U.K., since 2013.

Albert Munoz received the B.S. degree in chemical engineering and the M.B.A. degree from the Florida Institute of Technology, Melbourne, FL, USA, in 1999 and 2001, respectively, and the M.Sc. degree in environmental engineering and the Ph.D. degree in supply chain management from the University of Wollongong, Wollongong, NSW, Australia, in 2004 and 2012, respectively.

From 2009 to 2011, he was a Research Fellow with the SMART Infrastructure Facility, University of Wollongong, where he was appointed as a Lecturer in 2012. He has coauthored papers in risk, resilience, and robustness of systems under disruption threats. His research interests are in the measurement of risk in dynamic systems.

Katina Michael (Senior Member, IEEE) received the Bachelor of Information Technology degree from the School of Mathematical and Computing Science, University of Technology, Sydney, NSW, Australia, in 1996, the Doctor of Philosophy degree in information and communication technology from the Faculty of Informatics, University of Wollongong, Wollongong, NSW, Australia, in 2003, and the Master of Transnational Crime Prevention degree from the Faculty of Law, University of Wollongong in 2009.

She currently holds a joint appointment as a Tenured Professor with the School for the Future of Innovation in Society and the School of Computing, Informatics and Decision Systems Engineering, Arizona State University, Tempe, AZ, USA, where she is also the Director of the Society Policy Engineering Collective. She has held visiting academic appointments with Nanjing University, Nanjing, China, and the University of Southampton, Southampton, U.K. She was previously employed as a Senior Network Engineer with Nortel Networks, Ottawa, ON, Canada, from 1996 to 2001. She has also worked as a Systems Analyst with Andersen Consulting, Dublin, Ireland, and OTIS Elevator Company, Farmington, CT, USA. She has published six edited books, as well as coauthored a 500 page reference volume: *Innovative Automatic Identification and Location Based Services: From Bar Codes to Chip Implants* (Hershey, PA, USA: IGI, 2009). She has published over 200 peer-reviewed papers. She researches predominantly in the area of emerging technologies, and has secondary interests in technologies used for national security and their corresponding social implications.

Dr. Michael awarded the Brian M. O'Connell Distinguished Service Award in IEEESs Society for the Social Implications of Technology in 2017. He has been the Guest Editor of 15 special issues, including in the PROCEEDINGS OF THE IEEE, *Computer*, *IEEE Robotics & Automation Magazine*, IEEE POTENTIALS, *Journal of Location-Based Services*, *Computer Communications*, *Electronic Commerce Research*, and *Prometheus*. She was the Editor-in-Chief of the *IEEE Technology and Society Magazine* from 2012 to 2017, and has been the Senior Editor of the *IEEE Consumer Electronics Magazine* since 2015. She is the Founding Editor-in-Chief of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY.